编号：FGBGJ[2012]287CPFA-07

国家下一代互联网信息安全专项

下一代互联网网络病毒监控系统

（VDS）测评方案

编制：_____

审核：_____

批准：_____

2012-05-25 发布　　2012-06-01 实施

公安部计算机病毒防治产品检验中心

（天津市质量监督检验站第七十站）

目　录

1 测试说明

1.1 测试目的

为了贯彻落实国务院关于加快我国下一代互联网发展的工作部署，进一步提升下一代互联网信息安全产品的技术水平，保障国家发展改革委决定组织实施的2012年国家下一代互联网信息安全专项的顺利开展，根据《国家发展改革委办公厅关于组织实施2012年国家下一代互联网信息安全专项有关事项的通知》（发改办高技[2012]287号）中对“下一代互联网网络病毒监控系统”的相关要求，特制订本测评方案。

1.2 功能测试

1.2.1 基于海量病毒规则过滤

被测设备应具有离线的海量病毒规则库，病毒检测能力应达到GA243-2000《计算机病毒防治产品评级准则》中合格品要求。

1.2.2 在包和流层次的病毒传输和各种行为的检测能力

被测设备应支持HTTP协议、FTP协议、SMTP协议、POP3协议的病毒检测能力，并具有对病毒在网络上扫描、下载恶意程序、非法外联、接受或实施远程控制等行为的检测能力。

1.2.3 可疑文件样本的缓存和可疑源捕获

被测设备应能还原并缓存基于可还原明文协议的可疑样本，并记录可疑源的原始地址。

1.2.4 配置管理

可以通过WEB等方式对被测设备进行集中的管理与配置。

1.2.5 鉴别和授权

被测设备应具有防止非授权用户访问的控制功能，并严格限定被授权用户；同时应具有权限管理功能。

1.2.6 控制和通信安全

被测设备之间的控制和通信应具有加密传输的功能，确保安全性。

1.2.7 登录和报警

被测设备用户登录的信息应当及时记入日志，具有登录超时保护、自动锁定功能。

被测设备的报警信息应当及时记入日志，并便于查询，系统可以通过控制台、声音、邮件等方式进行报警。

1.2.8 碎片包处理

被测设备可以识别碎片包，并可以对碎片包进行处理。

1.2.9 阻断过滤

被测设备可以支持并接方式的阻断过滤。

1.2.10 用户访问控制

被测设备应能根据用户身份、用户网络地址等对用户的访问进行控制。

1.2.11 畸形报文检测功能

被测设备可以识别畸形报文，并可以对畸形报文进行处理。

1.2.12 支持对病毒事件的统一管理

被测设备应具有管理平台，应能对病毒事件进行统一管理。

1.2.13 万兆网络环境的支持能力

被测设备应支持万兆网络环境，负荷量不小于 20Gbps。

1.3 EAL3 评估

依据 GB/T 18336.3-2008《信息技术 安全技术 信息技术安全性评估准则 第 3 部分 安全保证要求》进行评估。

1.4 自主知识产权

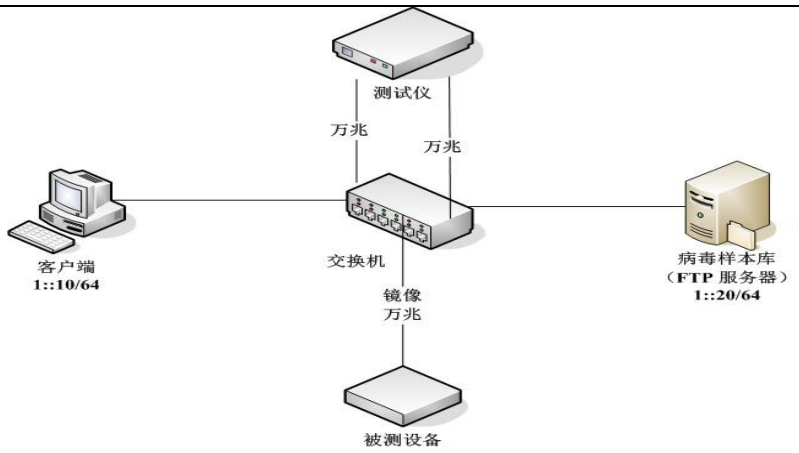
通过测试，判定厂商对自身产品源码的自主掌握程度。

2 功能与性能测试方案

2.1 基于海量病毒规则过滤

2.1.1 海量病毒检测测试

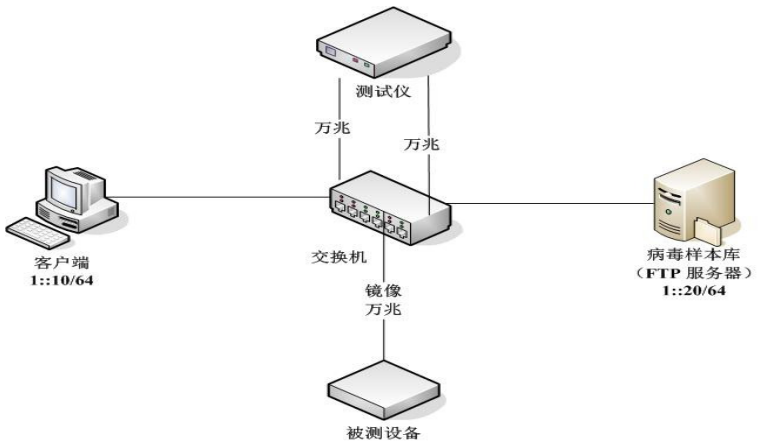
测试内容	被测设备能否检测海量病毒样本库中的样本文件
测试网络拓扑	

	
测试步骤	1. 按照上述拓扑图搭建测试环境，并分别对客户端、FTP 服务器的 IP 地址进行配置:客户端 IP 地址为 1::10/64、FTP 服务器 IP 地址为 1::20/64； 2. 开启测试仪，发送 10Gbps 的背景流量； 3. 将被测设备的病毒检测功能开启； 4. 配置完成后，在客户端上使用 FTP 客户端软件访问 FTP 服务器并下载病毒样本文件。
预期结果	可以检测病毒样本库中的样本文件，海量病毒样本库检测率>90%。
实际测试结果	□ 符合　　□ 不符合
备注	

2.2　在包和流层次的病毒传输和各种行为的检测能力

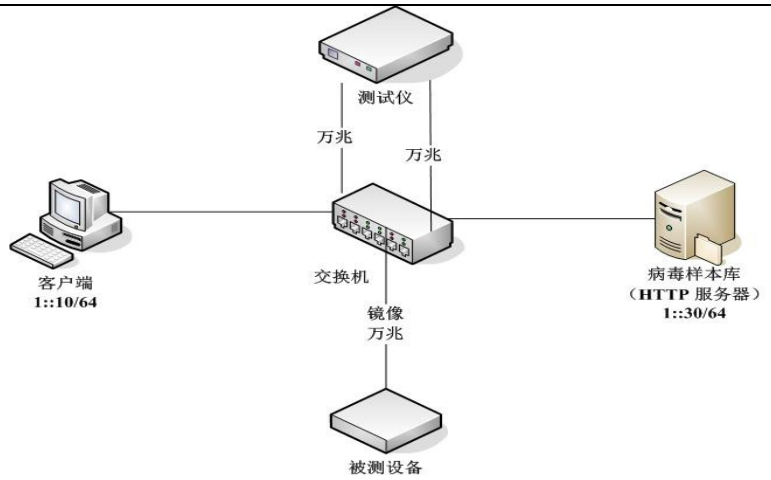
2.2.1　流检测能力测试

2.2.1.1　　FTP 协议下病毒检测

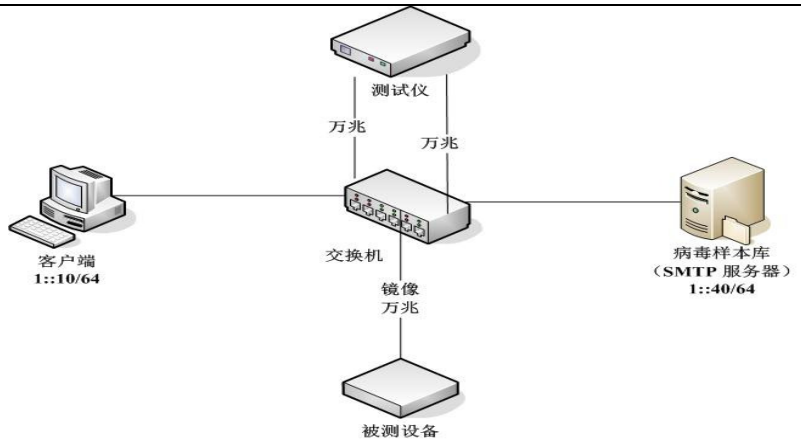
测试内容	FTP 协议下被测设备能否检测病毒样本库中的样本文件
测试网络拓扑	

测试步骤	1. 按照上述拓扑图搭建测试环境，并分别对客户端、FTP 服务器的 IP 地址进行配置:客户端 IP 地址为 1::10/64、FTP 服务器 IP 地址为 1::20/64； 2. 开启测试仪，发送 10Gbps 的背景流量； 3. 将被测设备的病毒检测功能开启； 4. 配置完成后，在客户端上使用 FTP 客户端软件访问 FTP 服务器并下载病毒样本文件。
预期结果	可以检测病毒样本库中的样本文件，病毒样本基本库检测率>85%，流行病毒样本库检测率>90%，特殊格式病毒样本库检测率>80%。
实际测试结果	□ 符合 □ 部分符合 □ 不符合
备注	

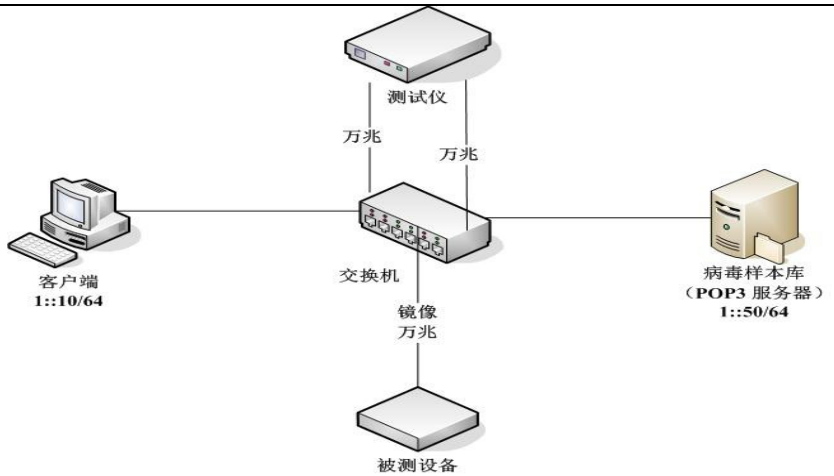
2.2.1.2 HTTP 协议下病毒检测

测试内容	HTTP 协议下被测设备能否能够检测病毒样本库中的样本文件
测试网络拓扑	
测试步骤	1. 按照上述拓扑图搭建测试环境，并分别对客户端、HTTP 服务器的 IP 地址进行配置:客户端 IP 地址为 1::10/64、HTTP 服务器 IP 地址为 1::30/64； 2. 开启测试仪，发送 10Gbps 的背景流量； 3. 将被测设备的病毒检测功能开启； 4. 配置完成后，在客户端上使用 HTTP 客户端软件访问 HTTP 服务器并下载病毒样本文件。
预期结果	可以检测病毒样本库中的样本文件，病毒样本基本库检测率>85%，流行病毒样本库检测率>90%，特殊格式病毒样本库检测率>80%。
实际测试结果	□ 符合 □ 部分符合 □ 不符合
备注	

2.2.1.3 SMTP 协议下病毒检测

测试内容	SMTP 协议下被测设备能否能够检测病毒样本库中的样本文件
测试网络拓扑	
测试步骤	1. 按照上述拓扑图搭建测试环境，并分别对客户端、SMTP 服务器的 IP 地址进行配置:客户端 IP 地址为 1::10/64、SMTP 服务器 IP 地址为 1::40/64； 2. 开启测试仪，发送 10Gbps 的背景流量； 3. 将被测设备的病毒检测功能开启； 4. 配置完成后，在客户端上使用 SMTP 客户端软件向 SMTP 服务器发送带有基本库病毒样本文件作为附件的邮件。
预期结果	可以检测病毒样本库中的样本文件，病毒样本基本库检测率>85%，流行病毒样本库检测率>90%，特殊格式病毒样本库检测率>80%。
实际测试结果	□ 符合　　□ 部分符合　　□ 不符合
备注	

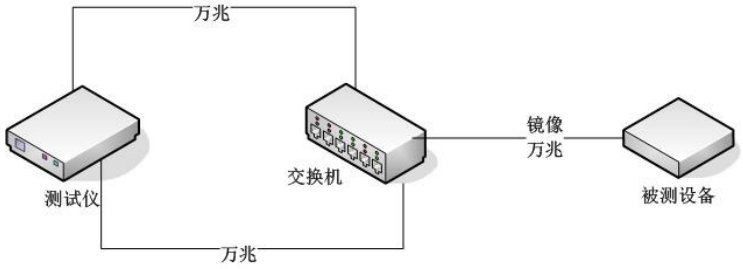
2.2.1.4 POP3 协议下病毒样本检测

测试内容	POP3 协议下被测设备能否能够检测病毒样本库中的样本文件
测试网络拓扑	
测试步骤	1. 按照上述拓扑图搭建测试环境，并分别对客户端、POP3 服务器的 IP

	地址进行配置:客户端 IP 地址为 1::10/64、POP3 服务器 IP 地址为 1::50/64； 2. 开启测试仪，发送 10Gbps 的背景流量； 3. 将被测设备的病毒检测功能开启； 4. 配置完成后，在客户端上使用 POP3 客户端软件从 POP3 服务器接收带有基本库病毒样本文件作为附件的邮件。
预期结果	可以检测病毒样本库中的样本文件，病毒样本基本库检测率>85%，流行病毒样本库检测率>90%，特殊格式病毒样本库检测率>80%。
实际测试结果	□ 符合 □ 部分符合 □ 不符合
备注	

2.2.2 包检测能力测试

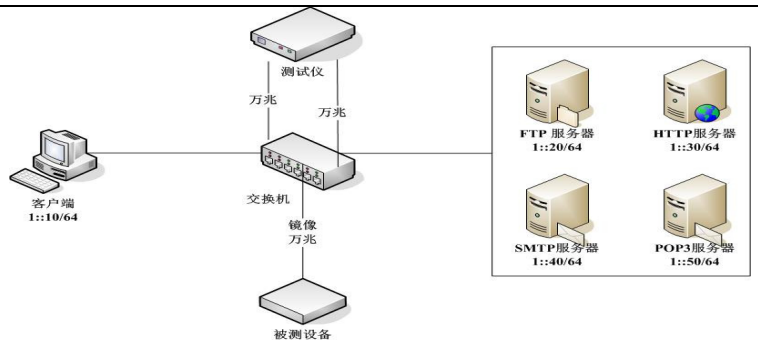
2.2.2.1 蠕虫检测

测试内容	被测设备能否检测蠕虫库中的样本文件
测试网络拓扑	
测试步骤	1. 按照上述拓扑图搭建测试环境 ； 2. 开启测试仪，导入蠕虫库中的样本文件，发送 10Gbps 的背景流量； 3. 将被测设备的病毒检测功能开启。
预期结果	可以检测蠕虫样本库中的样本文件。
实际测试结果	□ 符合 □ 不符合
备注	

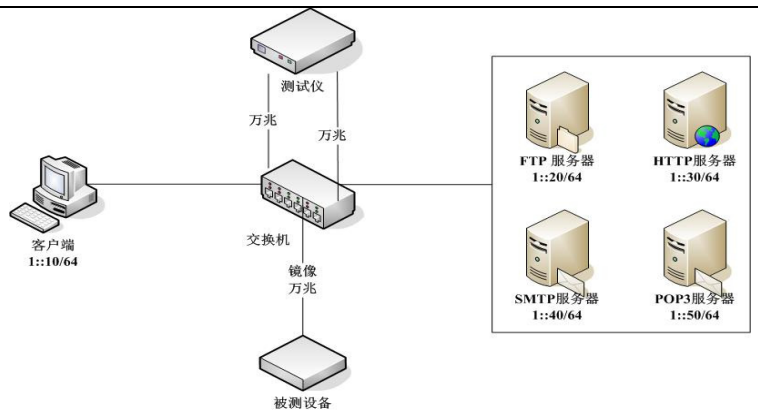
2.3 可疑文件样本的缓存和可疑源捕获

2.3.1 可疑样本缓存

测试内容	被测设备是否具有可疑样本缓存功能

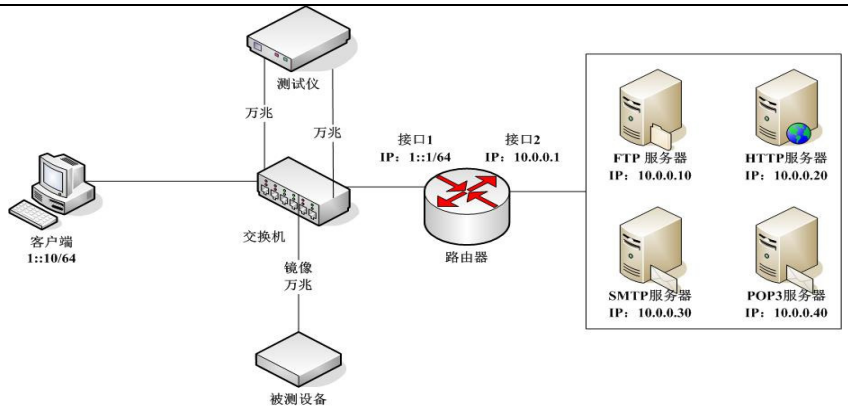
测试网络拓扑	
测试步骤	1. 按照上述拓扑图搭建测试环境，并分别对客户端、被测设备管理口的 IP 地址进行配置: a) 客户端 IP 地址为 1::10/64； b) FTP 服务器 IP 地址为 1::20/64； c) HTTP 服务器 IP 地址为 1::30/64； d) SMTP 服务器 IP 地址为 1::40/64； e) POP3 服务器 IP 地址为 1::50/64； 2. 开启测试仪，发送 10Gbps 的背景流量； 3. 开启被测设备的可疑样本的缓存功能； 4. 使用客户端用 HTTP 客户端、FTP 客户端、SMTP 客户端、POP3 客户端访问相应服务器，下载病毒样本； 5. 查看被测设备的缓存文件日志 6. 从样本缓存区将样本文件导出； 7. 计算导出的样本文件的 MD5 值，与原始样本文件进行比对。
预期结果	可以缓存样本文件，并与原始样本一致。
实际测试结果	□ 符合 □ 部分符合 □ 不符合
备注	

2.3.2 IPv6 网络可疑源捕获

测试内容	被测设备是否具有 IPv6 网络环境下的可疑源捕获功能
测试网络拓扑	

测试步骤	1. 按照上述拓扑图搭建测试环境，并分别对客户端、被测设备管理口的IP 地址进行配置: a) 客户端 IP 地址为 1::10/64； b) FTP 服务器 IP 地址为 1::20/64； c) HTTP 服务器 IP 地址为 1::30/64； d) SMTP 服务器 IP 地址为 1::40/64； e) POP3 服务器 IP 地址为 1::50/64； 2. 开启测试仪，发送 10Gbps 的背景流量； 3. 使用客户端用 HTTP 客户端、FTP 客户端、SMTP 客户端、POP3 客户端访问相应服务器，下载病毒样本； 4. 查看被测设备报警日志。
预期结果	可以准确记录病毒文件的来源。
实际测试结果	□ 符合 □ 部分符合 □ 不符合
备注	

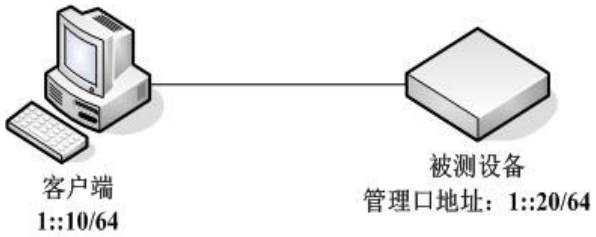
2.3.3 IPv6 与 IPv4 混合网络可疑源捕获

测试内容	被测设备是否具有 IPv6 和 IPv4 混合网络环境下的可疑源捕获功能
测试网络拓扑	
测试步骤	1. 按照上述拓扑图搭建测试环境，并分别对客户端、被测设备管理口的IP 地址进行配置: 1） 客户端 IP 地址为 1::10/64； 2） 路由器接口 1 的 IP 地址为：1::1/64； 3） 路由器接口 2 的 IP 地址为：10.0.0.1 4） FTP 服务器 IP 地址为 10.0.0.10； 5） HTTP 服务器 IP 地址为 10.0.0.20； 6） SMTP 服务器 IP 地址为 10.0.0.30； 7） POP3 服务器 IP 地址为 10.0.0.40；

	2. 开启测试仪，发送 10Gbps 的背景流量； 3. 使用客户端用 HTTP 客户端、FTP 客户端、SMTP 客户端、POP3 客户端访问相应服务器，下载病毒样本； 4. 查看被测设备报警日志。
预期结果	可以准确记录病毒文件的来源。
实际测试结果	□ 符合 □ 部分符合 □ 不符合
备注	

2.4 配置管理

2.4.1 Web 方式测试

测试内容	被测设备是否具有基于 Web 的配置管理方式
测试网络拓扑	
测试步骤	1. 按照上述拓扑图搭建测试环境，并分别对客户端、被测设备管理口的 IP 地址进行配置:客户端 IP 地址为 1::10/64、被测设备管理口 IP 地址为 1::20/64； 2. 使用 Web 客户端访问被测设备提供的 Web 管理地址。
预期结果	可以正常访问被测设备的 Web 管理界面。
实际测试结果	□ 符合 □ 不符合
备注	

2.5 用户鉴别和授权

2.5.1 用户身份鉴别

测试内容	被测设备是否具有用户身份鉴别功能
测试步骤	1. 用默认用户登录被测设备； 2. 增加一个新用户； 3. 用新用户登录被测设备。
预期结果	可以正常登录被测设备。
实际测试结果	□ 符合 □ 不符合
备注	

2.5.2 用户口令强度测试

测试内容	被测设备是否具有用户口令强度检查功能
测试步骤	1. 修改用户口令； 2. 使用位数小于 8 位的弱密码。
预期结果	被测设备提示口令强度不足。
实际测试结果	□ 符合 □ 不符合
备注	

2.5.3 Web 证书管理认证测试

测试内容	被测设备是否具有 Web 证书管理认证功能
测试步骤	1. 在被测设备上开启 Web 证书认证功能； 2. 在指定客户端安装相应证书； 3. 使用已安装证书的指定客户端登录系统； 4. 使用未安装证书的客户端登录系统。
预期结果	已安装证书的客户端可以正常访问，未安装证书的客户端无法访问。
实际测试结果	□ 符合 □ 不符合
备注	

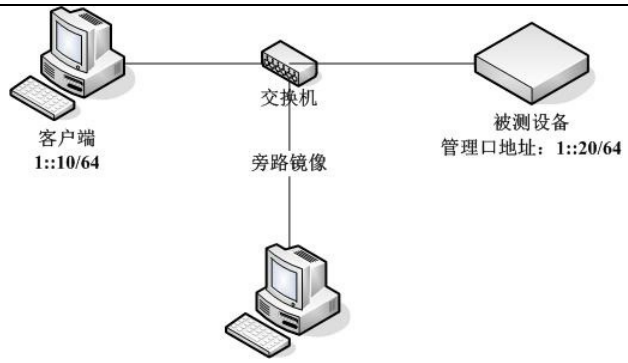
2.5.4 用户权限管理测试

测试内容	被测设备是否具有用户权限管理功能
测试步骤	1. 修改已有用户的权限，使其增加一个被授权功能； 2. 测试该用户是否能够正常访问被授权功能； 3. 修改已有用户的权限，删除其一个被授权功能； 4. 测试该用户是否能够访问刚刚被删除授权的功能。
预期结果	增加或删除相应权限后，用户可以或不可以访问的相应功能。
实际测试结果	□ 符合 □ 不符合
备注	

2.6 控制和通信安全

2.6.1 控制和通信安全

测试内容	被测设备是否具有加密通信的配置管理方式

测试网络拓扑	
测试步骤	1. 按照上述拓扑图搭建测试环境，并分别对客户端、被测设备管理口的 IP 地址进行配置:客户端 IP 地址为 1::10/64、被测设备管理口 IP 地址为 1::20/64； 2. 交换机配置一镜像口，复制测试设备和客户端之间的通信； 3. 使用 Web 客户端访问被测设备提供的 Web 管理地址； 4. 使用 Sniffer 客户端分析通信流量。
预期结果	控制和通信过程采用可靠的加密算法。
实际测试结果	□ 符合 □ 不符合
备注	

2.7 登录和报警

2.7.1 登录日志

测试内容	被测设备是否具有登录日志的记录功能
测试步骤	1. 开启被测设备的日志记录功能； 2. 用指定用户登录被测设备； 3. 查看登录日志，是否记录了上一步骤的用户登录信息。
预期结果	正常记录用户的登录信息
实际测试结果	□ 符合 □ 不符合
备注	

2.7.2 登录超时

测试内容	被测设备是否具有登录超时功能
测试步骤	1. 登录被测设备； 2. 开启被测设备的登录超时功能； 3. 设定登录超时时间； 4. 等待，无操作，直到超过超时时间范围； 5. 任意操作。
预期结果	被测设备应提示重新登录

实际测试结果	□ 符合 □ 不符合
备注	

2.7.3 登录锁定

测试内容	被测设备是否具有登录锁定功能
测试步骤	1. 登录被测设备； 2. 开启被测设备的登录锁定功能； 3. 设定登录锁定的次数条件和锁定时间； 4. 使用错误的用户名、密码登录，直到超过锁定条件； 5. 在锁定时间过后，重新用正确用户名、密码登录。
预期结果	登录被锁定，超过锁定时间后，用正确用户名、密码能正常登录。
实际测试结果	□ 符合 □ 不符合
备注	

2.7.4 报警日志

测试内容	被测设备是否具有报警日志记录功能
测试步骤	1. 登录被测设备； 2. 查看被测设备的报警日志；
预期结果	被测设备具有报警日志信息。
实际测试结果	□ 符合 □ 不符合
备注	

2.7.5 病毒检测日志

测试内容	被测设备的病毒检测日志功能是否完整
测试步骤	1. 登录被测设备； 2. 查看被测设备的病毒检测日志； 3. 是否记录病毒的文件名； 4. 是否记录病毒发送方和接收方的 IP 地址； 5. 是否记录病毒发送方和接收方的端口号； 6. 是否记录发现病毒的时间。
预期结果	被测设备具有较完整的病毒检测日志信息。
实际测试结果	□ 符合 □ 不符合
备注	

2.7.6 报警通知

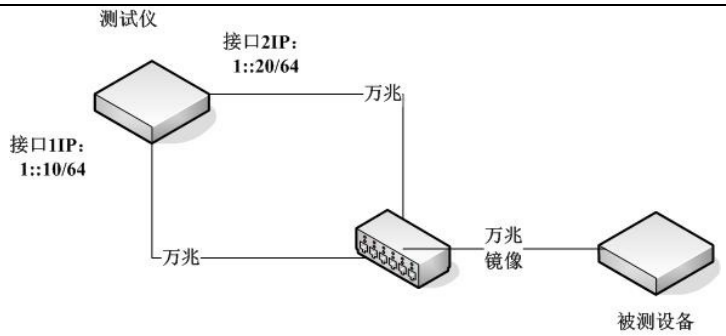
测试内容	被测设备是否具有报警通知功能
测试步骤	1. 登录被测设备； 2. 查看被测设备是否具有控制台、声音、邮件等报警通知功能；
预期结果	被测设备具有报警通知功能。
实际测试结果	□ 符合 □ 不符合
备注	

2.7.7 日志查询

测试内容	被测设备是否具有日志查询功能
测试步骤	1. 登录被测设备； 2. 查看被测设备是否可以对日志按日期、类型等条件进行查询。
预期结果	被测设备具有对日志的条件查询功能。
实际测试结果	□ 符合 □ 不符合
备注	

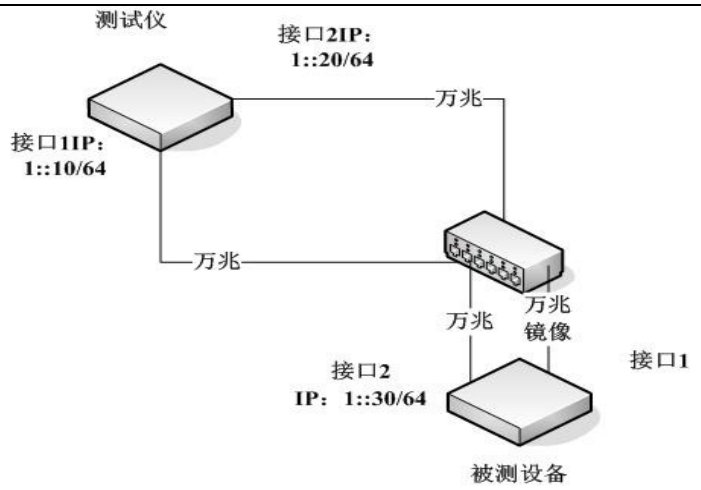
2.8 碎片包处理

2.8.1 碎片包的适当处理

测试内容	被测设备是否具有对碎片包的处理功能
测试拓扑	
测试步骤	1. 按照上述拓扑图搭建测试环境，将测试仪接口与对应被测设备的接口相连，配置测试仪接口 1 的 IP 地址为：1::10/64，接口 2 的 IP 地址为：1::20/64； 2. 配置交换机的镜像端口，复制测试仪接口 1 和接口 2 之间的流量； 3. 配置测试仪发送碎片数据包和正常数据包的混合网络流量。
预期结果	被测设备能够识别碎片包，并对其做相应的处理。
实际测试结果	□ 符合 □ 不符合
备注	

2.9 阻断过滤

2.9.1 并接方式发送拒绝包进行阻断

测试内容	被测设备是否支持并接方式的阻断过滤
测试拓扑	
测试步骤	1. 按照上述拓扑图搭建测试环境，并进行如下地址分配： 测试仪接口 1 的 IP 地址为：1::10/64； 测试仪接口 2 的 IP 地址为：1::20/64； 被测设备接口 1 设置为监听模式； 被测设备接口 2 的 IP 地址为：1::30/64； 2. 配置交换机的镜像口，镜像测试仪接口 1 与测试仪接口 2 之间的数据流量； 3. 开启被测设备的阻断功能； 4. 开启测试仪，从接口 1 向接口 2 持续发送带有病毒附件的 SMTP 协议数据流量； 5. 查看测试仪日志； 6. 查看被测设备阻断日志。
预期结果	被测设备能够识别并记录病毒来源，并采取 TCP Reset 或 ARP 欺骗等方式进行阻断。
实际测试结果	□ 符合 □ 不符合
备注	

2.10 用户访问控制

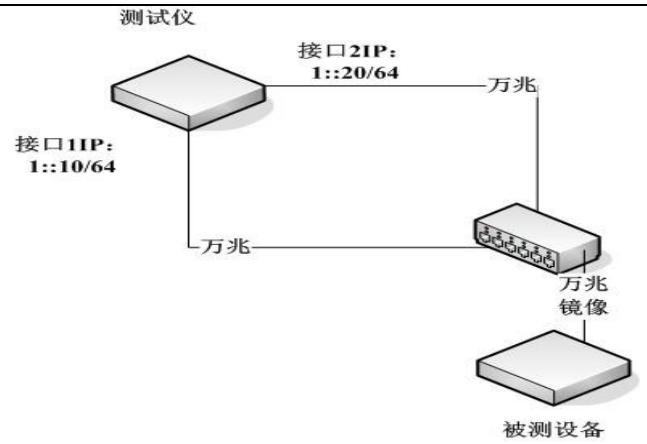
2.10.1 用户分组访问控制

测试内容	被测设备是否具有用户分组功能并依据分组进行访问控制
测试步骤	1. 用管理员身份登录被测设备的管理平台； 2. 新建用户 1 和用户 2，将用户 1 和用户 2 加入用户组 1； 3. 对用户组 1 分配相应权限；

	4. 使用用户 1 登录管理平台，查看相应功能； 5. 使用用户 2 登录管理平台，查看相应功能。
预期结果	用户 1 可以访问用户组 1 被授权的功能，不能访问用户组 1 未被授权的功能，用户 2 可以访问用户组 1 被授权的功能，不能访问用户组 1 未被授权的功能。
实际测试结果	□ 符合　　□ 不符合
备注	

2.11　畸形报文检测

2.11.1　畸形报文检测并处理

测试内容	被测设备是否具有对畸形报文的检测和处理功能
测试拓扑	
测试步骤	1. 按照上述拓扑图搭建测试环境，将测试仪接口与对应被测设备的接口相连，配置测试仪接口 1IP 地址为：1::10/64，接口 2IP 地址为：1::20/64； 2. 配置被测设备两个接口为交换模式或与之类似的模式； 3. 配置被测设备对畸形数据包的处理方式； 4. 配置测试仪构造畸形数据包； 5. 配置测试仪发送畸形数据包和正常数据包的混合网络流量； 6. 检查被测设备报警日志。
预期结果	被测设备具有与其配置相符的畸形数据包处理能力。
实际测试结果	□ 符合　　□ 部分符合　　□ 不符合
备注	

2.12　支持对病毒事件的统一管理

2.12.1　病毒事件的统计

测试内容	被测设备能否提供病毒事件的统计功能

测试步骤	1. 登录被测设备的管理平台； 2. 查看病毒事件的统计功能界面； 3. 查看各种病毒事件统计报表。
预期结果	被测设备能够提供比较丰富的病毒统计数据和统计报表
实际测试结果	□符合 □ 部分符合 □ 不符合
备注	

2.12.2 病毒事件的查询

测试内容	被测设备能否提供病毒事件的条件查询功能
测试步骤	1. 登录被测设备的管理平台； 2. 查看病毒事件的查询功能界面； 3. 输入以下几类条件进行查询： 1） 时间区间； 2） 病毒名； 3） 源 IP 地址； 4） 目的 IP 地址； 5） 源端口号； 6） 目的端口号； 7） 病毒文件名。
预期结果	被测设备能够提供与查询条件相符的查询结果
实际测试结果	□符合 □ 部分符合 □ 不符合
备注	

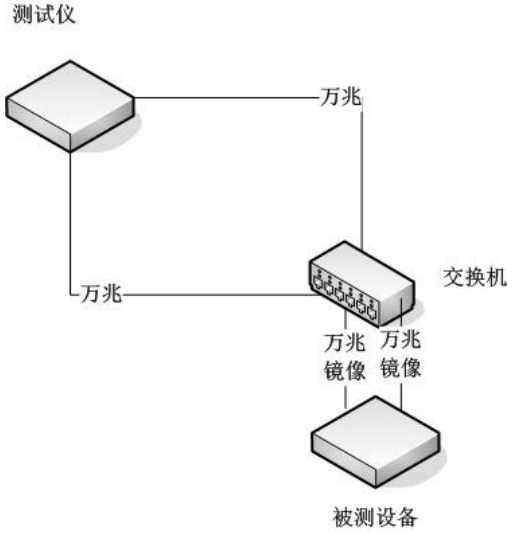
2.12.3 病毒事件的导出

测试内容	被测设备能否提供病毒事件的导出功能
测试步骤	1. 登录被测设备的管理平台； 2. 查看病毒事件的查询功能界面 3. 输入查询条件进行查询； 4. 导出查询结果； 5. 查看统计功能界面； 6. 导出统计报表和数据； 7. 打开导出的数据文件，与功能界面上的数据源进行比对。
预期结果	能够导出相应的事件数据，内容与查询结果和统计结果相符。
实际测试结果	□符合 □ 部分符合 □ 不符合

备注	

2.13 万兆网络环境的支持能力

2.13.1 万兆网络环境的支持能力

测试内容	被测设备是否具有万兆网络环境的支持能力
测试网络拓扑	
测试步骤	1. 根据以上拓扑图配置网络： 2. 配置测试仪的的万兆接口 1 与交换机的万兆接口 1 相连；万兆接口 2 与交换机的万兆接口 2 相连。 3. 配置交换机的万兆接口 3 镜像万兆接口 1 和万兆接口 2 的流量，万兆接口 4 也镜像万兆接口 1 和万兆接口 2 的流量。 4. 开启被测设备的病毒检测功能； 5. 使用测试仪将含有病毒的数据包和正常数据包混合，并以 10Gbps 高速发送； 6. 观察测试仪的结果。
预期结果	设备负荷量不小于 20Gbps，设备可以正常检测病毒事件。
实际测试结果	□符合 □ 部分符合 □ 不符合
备注	

3 EAL3 级测试

3.1 安全目标（ST）

3.1.1 ST 引言（ASE_INT.1）

测试内容	确认 ST 引言是否正确地标识了 ST，以及 ST 引言是否完备并与 ST 的其他部分保持一致。

测试方法与步骤	评估者检查 ST 的引言描述，确认开发者所提供的信息是否满足该子活动在内容和形式上的要求。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.1.2 TOE 描述 （ASE_DES.1）

测试内容	确认开发者在安全目标中对被测产品的描述是否包括了有助于理解被测产品目的和功能的信息，以及该描述是否完备和一致。
测试方法与步骤	1. ST 文档对被测产品的范围和边界的描述； 2. ST 文档对被测产品的描述时连贯的、内在一致的 ； 3. 评估者检查 ST 对被测产品的描述，确认开发者所提供的信息是否满足该子活动在内容和形式上的要求。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.1.3 安全环境（ASE_ENV.1）

测试内容	确认安全环境的陈述对有关被测产品与其预期应用环境的安全问题的定义是否清晰、连贯、一致。
测试方法与步骤	1. ST 文档在被测产品安全环境的陈述中标识并解释了所有的假设、所有的威胁和所有的组织安全策略； 2. 文档对被测产品安全环境的陈述是连贯的，内在一致的； 3. 评估者检查 ST 文档对被测产品安全环境的陈述，确认开发者所提供的信息是否满足上诉关于评估证据在内容和形式上的要求。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.1.4 安全目的（ASE_OBJ.1）

测试内容	确认安全目的描述是否完备和一致，并确认安全目的是否能对抗已标识的威胁，实现已标识的组织安全策略并遵循规定的假设。
测试方法与步骤	1. 安全目的的陈述是否定义了被测产品及其环境的安全目的； 2. 安全目的是否清楚地陈述了其目的可以追溯至由被测产品对抗的已标识的威胁； 3. 安全目的陈述是连贯的、内在一致的；

	4. 评估者检查 ST 文档对被测产品安全目的的陈述，确认开发者所提供的信息是否满足上诉关于评估证据在内容和形式上的要求。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合 □ 不符合
备注	

3.1.5 IT 安全要求（ASE_REQ.1）

测试内容	依据安全目的的陈述，检查开发者对被测产品或其环境应满足的 IT 安全要求（包括安全功能要求和安全保证要求）的定义，并确认作为被测产品开发的基础，是否充分地阐明了被测产品的安全要求和 IT 环境安全要求，且所阐明的内容是充分的。
测试方法与步骤	1. 开发者是否遵循国标 GB/T 18336 第二部分安全功能要求组件和第三部分安全保证要求组件的表达方式对 IT 安全要求进行了规范性的描述。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合 □ 不符合
备注	

3.1.6 明确陈述的 IT 安全要求（ASE_SRE.1）

测试内容	确认开发者在安全目标中描述或引用的 GB/T18336 第二部分或第三部分之外的 IT 安全要求是否恰当和充分。
测试方法与步骤	评估者检查开发者提供的关于为被测产品补充的安全功能要求，提取相应证据，检查安全目标对附加的安全功能要求是否采用 GB/T 18336 要求的模板格式进行标识，检查安全目标的基本原理部分，确认附加的安全功能要求是否是可用的。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合 □ 不符合
备注	

3.1.7 TOE 概要规范（ASE_TSS.1）

测试内容	依据安全要求的陈述，确认 ST 概要规范的陈述是否为被测产品安全功能和保证措施提供了清晰完整的高层定义，并且该定义满足 TOE 的安全要求。
测试方法与步骤	1. 评估者检查开发者提供的关于被测产品的安全功能和相关的保证措施，提取相应证据。

预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.1.8 PP 声明（ASE_PPC.1）

测试内容	PP 声明的评估。
测试方法与步骤	评估者确认开发者对于 ST 的 PP 声明。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.2 开发活动

3.2.1 功能规范 （ADV_FSP.1）

测试内容	确认开发者是否充分描述了被测产品的安全功能且其安全功能能否满足 ST 的安全功能要求。
测试方法与步骤	1. 功能规范文档应详细及完备地描述了被测产品的安全功能及其外部接口； 2. 功能规范文档是 TOE 安全功能要求的一个精确且完备的实例化； 3. 评估者检查被测产品功能规范文档关于对被测产品各项安全功能的定义、相关 IT 技术要求以及外部 TSF 接口的描述，确认开发者提供的信息是否满足该子活动在内容和形式上的要求： 4. 根据以上对证据的提取和相应的评估陈述，评估者确认《被测评产品（名称、版本号） 功能规范》文档是否正确并充分地描述了安全功能，确认其功能规范涵盖了 ST 中所有的安全功能，并且所有的安全功能都完全地映射到了功能规范的描述中； 5. 对于每个安全功能的外部接口，功能规范文档的描述和 ST 中 TOE 概要规范的描述是否一致。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.2.2 高层设计（ADV_HLD.2）

测试内容	确认开发者是否以主框架单元（例如：子系统）的方式描述了被测产品的安全功能，是否对构成被测产品的结构单元接口进行了描述，并说明该高层描述是功能规范的正确实现。

测试方法与步骤	1. 在结构上以主框架单元（例如：子系统）的方式描述被测产品安全功能； 2. 描述被测产品中每个主框架单元所提供的安全功能以及主框架单元之间的相互关系； 3. 标识被测产品安全功能所要求的任何基础性硬件、固件或软件，以及在这些硬件、固件或软件中实现的保护机制所提供的功能表示； 4. 描述每个主框架单元的接口、外部可见接口、提供对效果、异常和错误信息的详细描述； 5. 是否把被测产品分成 TSP 实施和其它子系统进行描述； 6. 评估者检查被测产品高层设计文档关于对被测产品主体框架和其结构单元以及外部安全功能接口的描述，确认开发者所提供的信息是否满足该子活动在内容和形式上的要求； 7. 评估者检查高层设计文档是否使用非形式化的自然语言描述被测产品在结构上实现功能规范所定义的各项安全功能及其安全机制； 8. 评估者检查在被测产品的高层设计中，开发者是否描述了每个子系统的接口，并标识了其外部接口，并对使用该接口的目的、使用方法进行了描述。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.2.3 表示对应性评估 （ADV_RCR.1）

测试内容	检查开发者提供的被测产品安全功能表示的所有相邻对之间的对应性分析，确认被测产品的开发者是否正确地、完整地实施了 ST、功能规范、高层设计的要求。
测试方法与步骤	1. 对应性分析文档应详细及完备地描述 TSF 表示的相邻对之间的对应关系，并且都依次得到了正确且完备的细化； 2. 评估者检查ST 文档中的被测产品概要规范和其功能规范之间的对应性分析，被测产品概要规范的安全功能和功能规范中的接口描述是否一致，两者提供的安全功能是否相同，TOE 功能规范中的接口是否是概要规范中安全功能的进一步细化； 3. 评估者检查被测产品的功能规范和高层设计之间的对应性分析，被测产品的功能规范中标识的各项安全功能是否都能够映射到高层设计中描述的 TSF 子系统中，对于每一项安全功能，是否都有相关的 TSF 子系统支持其功能；
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.3 指导性文档

3.3.1 管理员指南（AGD_ADM.1）

测试内容	确认指导性文档是否描述了如何以安全的方式管理被测产品。
测试方法与步骤	1. 管理员指南应描述管理员可使用的管理功能和接口，包括激活接口的方法，由管理员设置的参数及有效值、缺省值、即时的 TSF 响应或返回值； 2. 管理员指南应描述与管理员有关的 IT 环境的所有安全要求，以及在安全处理环境中必须进行控制的功能和权限的警告； 3. 管理员指南应描述与需要执行的管理功能相关的每一类安全相关事件，包括在安全功能控制下改变实体的安全特性； 4. 管理员是 TSF 所信任的，负责设置、维护和管理被测产品的相关人员； 5. 评估者检查被测产品指南文档是否标识并描述了管理员的职责、由管理员来控制的功能和特权，确切定义了每个安全功能的参数、参数的用途、参数的有效值和缺省值。评估者检查其是否描述了在管理员的控制下指定了适当安全值的所有安全参数； 6. 评估者检查被测产品管理员指南文档，并与安全目标中的相关内容进行对比和分析，确认管理员指南文档是否与其他文档保持一致；
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合 □ 不符合
备注	

3.3.2 用户指南（AGD_USR.1）

测试内容	确认用户指南是否描述了 TSF 提供的安全功能和接口，以及用户指南是否提供了安全使用被测产品的说明。
测试方法与步骤	1. 用户指南应描述用户可使用的管理功能和接口，包括激活接口的方法，由用户设置的参数及有效值、缺省值、即时的 TSF 响应或返回值； 2. 用户指南应描述与用户有关的 IT 环境的所有安全要求，以及受安全环境所控制的用户可访问的功能和权限的警告； 3. 用户指南应描述用于被测产品安全运行所必须的用户职责； 4. 通过检查被测产品的用户指南，评估者确认其是否描述了用户可执行的各种命令，即用户接口处提供的可见安全功能，并确切标识和解释了每一个命令的定义、用途。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合 □ 不符合
备注	

3.4 测试活动

3.4.1 测试范围（ATE_COV.2）

测试内容	确认测试是否能充分保证 TSF 已经按照功能规范被系统的测试过。
测试方法与步骤	1. 《被测评产品（名称、版本号）测试文档》应当论证测试文档中所标识的测试和功能规范中所描述的 TSF 之间的对应性； 2. 《被测评产品（名称、版本号）测试文档》应当论证功能规范中所描述的 TSF 和测试文档中所标识的测试之间的对应性是完全的； 3. 评估者检查《被测评产品（名称、版本号）测试文档》中测试分析部分对被测产品的测试范围陈述，确认开发者所提供的信息是否满足上述关于评估的内容和形式上的要求； 4. 在测试范围分析文档中，开发者应概括测试项目与功能规范中描述的安全功能之间的对应关系； 5. 通过检查测试范围分析中列出的测试和安全功能之间的对应性，评估者检查测试文档中列出的测试用例与功能规范是否是一致的；
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.4.2 测试深度（ATE_SPT.1）

测试内容	确认开发者是否已经对照高层设计测试了 TSF。
测试方法与步骤	1. 《被测评产品（名称、版本号） 测试文档》应当论证测试文档中所标识的测试足以论证被测产品的 TSF 运行和高层设计是一致的； 2. 评估者检查测试文档对被测产品测试深度的陈述，确认开发者所提供的信息是否满足上述关于评估的内容和形式上的要求； 3. 在测试深度分析文档中，开发者应描述测试与高层设计子系统之间的对应关系，每个安全功能子系统都进行了测试。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.4.3 功能测试（ATE_FUN.1）

测试内容	确认开发者的安全功能测试文档是否表明所有安全功能都按规定所实现。
测试方法与步骤	1. 《被测评产品（名称、版本号） 测试文档》应提供测试计划、测试程序的描述，预期的测试结果和实际的测试结果； 2. 《被测评产品（名称、版本号） 测试文档》中的测试计划应标识测试的安全功能，描述要执行的测试目标；

	3. 《被测评产品（名称、版本号） 测试文档》中的测试过程描述应当标识要执行的测试，并描述每个安全功能的测试概括； 4. 《被测评产品（名称、版本号） 测试文档》的预期测试结果应当表明成功测试运行后的预期输出； 5. 《被测评产品（名称、版本号） 测试文档》中开发者执行测试的结果应当论证每个被测试的安全功能已按照规定运行； 6. 评估者检查测试报告中对被测产品的测试陈述，确认开发者所提供的信息是否满足上述关于评估的内容和形式上的要求。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合 □ 不符合
备注	

3.5 脆弱性活动

3.5.1 误用（AVA_MSU.1）

测试内容	确认指南文档中没有误导的、不合理的和冲突的指导信息，指导性文档已经对所有操作方式提供了安全规程，以及使用指南能够防止和检测到不安全的 TOE 状态。
测试方法与步骤	1. 指导性文档完备、清晰地描述 TOE 所有可能的运行方式； 2. 指导性文档陈述所有目标环境的假设以及外部安全措施； 3. 指导性文档的完备性、合理性、一致性； 4. 评估者检查开发者提供的指导性文档、对指南的误用分析文档和其他评估证据，检查开发者在指南文档中是否描述了被测产品所有可能的运行方式。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合 □ 不符合
备注	

3.5.2 安全功能强度（AVA_SOF.1）

测试内容	确认在 ST 中是否为所有概率论或排列组合机制作出 SOF 声明，以及开发者的 SOF 是否被正确的分析。
测试方法与步骤	1. 开发者对 TOE 安全功能强度分析应说明其安全机制达到或超过了定义的最低强度； 2. 评估者检查 ST 文档中关于被测产品概要规范的陈述，检查被测产品概要规范是否具有概要或排列组合建立的机制以安全功能强度（SOF）定级的形式。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。

实际测试结果	□ 符合　　□ 不符合
备注	

3.5.3 脆弱性分析（AVA_VLA.1）

测试内容	确认开发者进行了脆弱性分析确定明显的安全脆弱性的存在， 并确认在所期望的环境下脆弱性不能被利用。
测试方法与步骤	1. 被测评产品（名称、版本号） 脆弱性分析》应该分析被测产品的脆弱性，对每个已经确认的脆弱性进行描述，给出该脆弱性在预期环境中不可利用的合理解释； 2. 开发者对被测产品脆弱性的分析应与 ST 文档及指南文档保持一致性； 3. 评估者检查开发者提交的被测产品脆弱性分析文档是否包括被测产品脆弱性分析的证据的内容和形式的信息，是否给出了脆弱性在预期环境中不可利用的必要解释；
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.6 生命周期支持

3.6.1 开发安全（ALC_DVS.1）

测试内容	确认开发者对开发环境的安全控制，并且确认这些安全措施能否为被测产品设计、生产和维护中的机密性和完整性提供必要的保护。
测试方法与步骤	1. 开发安全描述部分应详细描述应用于开发环境中采用的物理、程序、人员以及其他方面的安全措施，并提供执行这些安全措施产生的证据； 2. 到开发现场核查被测评公司对安全措施的实施情况； 3. 开发安全是为了保护 TOE 及其相关信息，防止它们收到干扰和暴露，开发过程中的干扰使故意引入脆弱性成为可能，而设计信息的暴露可能导致脆弱性更容易被人利用，最终导致 TOE 的机密性和完整性受到破坏。开发环境安全包括开发场地的物理安全、逻辑安全以及人员安全，涉及到在开发环境中采用的物理、程序、人员以及其他方面的安全措施；
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.7 配置管理

3.7.1 CM 能力（ACM_CAP.3）

测试内容	确认开发者是否清晰的定义了被测产品和它的相关配置项，以及改变这些配置项的能力是否被适当的控制。
测试方法与步骤	1. 配置管理文档应描述CM系统中的每一配置项的唯一标识及标识配置项的方法： 2. 配置管理文档应描述CM系统的使用方法及如何使用CM系统以维护配置项的完整性； 3. 评估者检查开发者是否通过配置管理工具对被测产品的研发进行了有限的管理，开发者是否提交了CM清单和CM计划。CM文档中是否明确地定义了被测产品的所有配置项，提供了跟踪任何变化的方法和对操作的授权规则。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合 □ 不符合
备注	

3.7.2 CM范围（ACM_SCP.1）

测试内容	确认开发者是否至少按照被测产品的实现表示、设计、测试、用户和管理员指南、CM文档以及安全缺陷执行了配置管理。
测试方法与步骤	1. CM系统跟踪的所有必需的配置项； 2. CM文档应描述CM系统如何跟踪配置项的方法； 3. 评估者检查被测产品的配置清单，配置清单是否列出了生命周期各阶段生成的开发、设计、测试等文档及代码，是否包括满足评估要求的EAL3保证级所需的全部文档； 4. 评估者确认文档是否描述了在被测产品的整个生命周期中如何标识配置项以及追踪每个配置项状态的方法和规程。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合 □ 不符合
备注	

3.8 交付和运行

3.8.1 交付（ADO_DEL.1）

测试内容	提供给用户时的交互文档应描述用于保持被测产品完整性的所有程序。
测试方法与步骤	1. 交付文档应描述用以维护安全所必需的所有程序； 2. 评估者检查开发者是否将被测产品交付给用户的程序完整地程序化；在给用户方分发被测产品不同版本时，用以维护安全所必需的所有程序是否都在交付文档中得以充分的描述，在实际运用中得以确切的执行。
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。

实际测试结果	□ 符合　　□ 不符合
备注	

3.8.2 安装、生成和启动（ADO_IGS.1）

测试内容	确认被测产品的安全安装、生成和启动的程序和步骤都已文档化，并最终形成安全配置。
测试方法与步骤	安装生成和启动文档应描述被测产品在期望的安全方式下安装、生成和启动所必需的步骤；
预期结果	如果开发者提供的文档描述不满足项目要求，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.9 独立性测试

测试内容	TOE 安全功能执行的正确性。
测试方法与步骤	1. 开发者应提供一个与开发者的安全功能测试中使用的资源相当的合集； 2. 评估者参考开发者提供的测试文档形成抽样子集；（如攻击行为监测、数据分析、安全告警等） 3. 评估者依据测试子集设计测试用例，验证 TOE 安全功能执行的正确性与评估证据的一致性，确保产品安全功能按照规定执行。
预期结果	如果开发者未提供文档，或产品 TOE 安全功能不一致，则本项判为不符合。
实际测试结果	□ 符合　　□ 不符合
备注	

3.10 渗透性测试

测试内容	根据脆弱性分析文档进行渗透性测试。
测试方法与步骤	1. 开发者应提供脆弱性分析文档，描述产品可以存在的每一个脆弱性； 2. 安全漏洞测试 针对可能实施的脆弱性和渗透性测试方法，对其实现手段进行简单介绍。其中网络脆弱性测试主要针对对象是提供服务的宿主主机，Web 应用脆弱性测试主要针对对象是现有的 Web 应用服务。 1） 网络脆弱性测试 探测工具：脆弱性扫描工具、审计网络用的安全分析工具等。 渗透工具集：包括针对各种操作系统和数据库的溢出渗透工具、口令破解工具等。 2） Web 应用脆弱性测试

	探测工具：Web 应用安全扫描器（如明鉴 Web 应用弱点扫描器），针对 Web 应用渗透性测试主要分为：注入检测、跨站脚本攻击检测、Web 认证攻击检测、会话管理攻击、信息泄露检测（源代码、目录信息）等。 渗透验证：可通过扫描工具或手工调用浏览器验证 Web 应用漏洞，如利用 SQL 注入点获取后台数据库相关信息。 3. 抗攻击测试 采用攻击工具或专用性能检测设备，对产品进行各种拒绝服务攻击，攻击手段至少包括 Syn Flood、UDP Flood、Ping of Death 以及分布式拒绝服务攻击，检查产品是否能够抵御相应攻击。
预期结果	如果产品未提供文档，或产品存在脆弱性（如漏洞、未申明端口等），则本项判为不符合。
实际测试结果	□ 符合 □ 不符合
备注	

3.11 自主知识产权

测试内容	对厂家产品代码同业界已有产品代码进行比较，检测厂家产品的自主知识情况。
测试方法与步骤	1. 要求厂家以源代码的形式提供产品代码，并提供证明产品代码已经通过 CheckStyle、StyleCop 等代码格式审查工具的检查，格式符合代码相似度检查的要求； 2. 要求厂家在独立干净的机器上进行源代码的编译和生成，并能够对应到已经部署的软硬件设备上的实际执行代码； 3. 使用 black duck 工具对产品的源代码（关键核心模块）进行对比分析测试，得到相似程度； 4. 相似分析结果应符合自主原创测评指南的要求。
预期结果	如果厂家能够提供正确的、通过代码格式审查的产品源代码，且代码相似分析结果符合自主原创测评指南的要求，则此项为符合项。
实际测试结果	□ 符合 □ 不符合
备注	